RISK MANAGEMENT
PLANNING FOR UNCERTAINTY
CONTENTS

1.0 INTRODUCTION: RISK MANAGEMENT OVERVIEW 3
  1.1 What is a risk? 3
  1.2 Risk Management 4
  1.3 Risk Response Strategies 4
    1.3.1 Accept 4
    1.3.2 Avoid 4
    1.3.3 Transfer 4
    1.3.4 Mitigate 5
  1.4 Risk Types 5
    1.4.1 Safety 5
    1.4.2 Security 5
    1.4.3 Performance 5
    1.4.4 Cost 5
    1.4.5 Schedule 6
  1.5 Risk of Not Implementing Risk Management in an Organization or Project 6

2.0 RISK MANAGEMENT PLANNING 7
  2.1 Risk Management Implementation Plan 7
  2.2 Purpose 7
  2.3 Scope 7
  2.4 Roles and Responsibilities 7
  2.5 Tools 9
  2.6 Communicating Risk 9
  2.7 Risk Identification and Management Process 9
    2.8 Risk Analysis (Probability/Likelihood and Consequence/Criticality) 11
      2.8.1 DOD Analysis and Risk Reporting Matrix 11
      2.8.2 FAA Analysis and risk reporting matrix 12
  2.9 Risk Response: Mitigation Planning 13
  2.10 Risk Monitoring 13

3.0 RISK MANAGEMENT IMPLEMENTATION 14
  3.1 Risk Management Board or Committee Charter 14
  3.2 Making it Happen! 15

4.0 ACRONYMS 16

5.0 REFERENCES 16

6.0 STAKEHOLDER FEEDBACK 16

7.0 DISTRIBUTION / COMMUNICATION 16

PURPOSE:
This document provides an overview of risk management using commercial and government examples, and Department of Defense, Federal Aviation Administration, and Project Management Institute guidance. It outlines steps to identify risk, perform root cause analysis, and initiate response planning; and recommends steps to implement risk management within an organization.

SCOPE:
Risk management practices apply to anyone involved in managing uncertainty of outcomes where safety, security, performance, cost, and schedule are factors. Risks may be negative with detrimental impacts or positive where opportunities such as increased sales and revenue occur. Risk responses include: avoid, transfer, accept, and mitigate. This document provides a general overview of risk management with primary focus on negative risks and mitigation.
1.0 INTRODUCTION: RISK MANAGEMENT OVERVIEW

An effective risk management program begins with clearly defined requirements and assessment, and includes risk analysis and planning. It is understood and genuinely committed to by the organization’s management and leadership. The understanding and commitment of an organization’s management and leaders ensures adequate resources and decisions in order to minimize the likelihood of disruption and maximize the probability of delivering desired products and outcomes.

The risk management process is an integrated collection of principles, policies, processes, and procedures, and programs used to identify, analyze, assess, management, and monitor risk. An effective risk management process requires the support and commitment of the entire project or product team, including stakeholders, Government and contractor program offices, program teams, support personnel, and subject matter experts (SME). Clear roles and responsibilities are a primary consideration.

An organization’s culture and value system will determine the emphasis placed on risk management and the degree of tolerance placed on varying types of risk. Safety is a primary focus of the Federal Aviation Administration (FAA). Network infrastructure and security are top priorities of the Department of Defense (DOD) to ensure messages get to theatre expeditiously and securely. Quality produce, cleanliness, worker safety, and good customer service are priorities in food industry. Concrete mix, temperature, and humidity are considerations in construction. Each of these entities requires strong risk management programs and processes to minimize incidents and maximize effectiveness of their mission and objectives.

1.1 WHAT IS A RISK?

Risk is uncertainty of outcomes in a situation. It is an event that may occur when triggered by a specified antagonist or action. The action taken to manage a risk is called a response. Until the trigger occurs, steps may be able to be put in place to eliminate or reduce risk (prevent the trigger from occurring). The likelihood that a risk will occur is referred to as probability. The degree of criticality of potential impact may be called the consequence. A risk that becomes an actuality, which means the event occurred, is an issue. The following is a list of risk examples identified as “if” “then” statements, a common method used to describe risk and impact.

• If I walk on an icy sidewalk, then I may fall.
• If you speed, then you may get a speeding ticket.
• If there is no virus software installed on a computer, then data may be compromised.
• If the company’s IT infrastructure is compromised, then personal identifiable information may be accessed.
• If a Department of Defense network is compromised, then troops may die or missions disrupted.
• If the kitchen floor is greasy, then workers may slip and fall.
• If you purchase lesser quality produce or merchandise, then you may lose customers.
• If you talk on a cell phone while operating heavy machinery, then an accident may happen.
• If concrete is poured when the temperature is below acceptable, then curing will be disrupted and the resulting product will fail.
• If a company can’t retain qualified personnel, then service level agreements may not be met.
• If the Government continues executing contracts based on least priced technically acceptable bids, then the quality of service of those agencies may decrease.
• If TSA airport security equipment fails, then a hijacker may blow up a plane.
1.2 RISK MANAGEMENT

Risk management is “the process of defining how to conduct tasks or activities to ensure that the degree, type, and visibility of risks are commensurate with the risks themselves and commensurate with the importance of the project to the organization”. It is the act of planning for risk and taking the steps necessary to identify, assess, perform root cause analysis, respond by taking action, and then monitoring and controlling those actions to ensure desired outcomes.

Organizations that exercise good risk management, review risks on a regular basis and generally assign an individual or individuals as primary “Risk Manager(s)” to consistently provide guidance and support to teams and stakeholders in the identification, monitoring, and reporting of risks. Risk management committees or boards provide leadership oversight of the risk program, risk escalation, and decisions.

1.3 RISK RESPONSE STRATEGIES

When we implement strategies to deal with risks we may choose to accept risk, avoid the risk, transfer or shift the impact to a third party, or take action to mitigate and reduce the risk.

1.3.1 ACCEPT

When accepting risk, an organization acknowledges that the risk event or condition may be realized and willingly accepts the risks with the consequences.

• If I speed, then I may get a speeding ticket. By choosing to speed, I accept the consequences of a fine or possible accident and fatal injury. I assess my rate of speed over the acceptable limit and the probability of being caught together with the criticality of the possible consequences and choose.

• In theatre, messages are required to be delivered securely and expeditiously. Given a choice of delivering a message with one or the other both carry high probability of negative outcomes. I can get a message to troops expeditiously but unsecure, and secure but slowly. If a message stating that reinforcements are on their way arrives quickly, but the message is unsecured, then the enemy has a chance of changing maneuvers and intercepting the reinforcements. If the message is secure, but comes too late, then troops could change direction or tactics and relocate and miss the opportunity to join reinforcements altogether, or fail to move and be blown up with the enemy.

• Choosing one over the other is acceptance of consequences.

1.3.2 AVOID

Risk avoidance includes the activities of eliminating risk altogether.

• If I choose not to walk on an icy sidewalk then there is no risk of slipping and falling.

• If a heavy equipment operator chooses not to talk on the phone while operating his equipment then he is avoiding an accident that would have cell phone use as “root cause”.

• Contractors choose “not” to pour concrete in colder weather or other unfavorable conditions to avoid consequences of rework, or failed product. A delay in schedule as a result may not always result in lost equity. Risk owners need to assess impacts, probability and criticality, and choose wisely.

1.3.3 TRANSFER

By choosing a least priced technically acceptable contract the Government transfers the risk that lower cost could mean lower quality, to the contractor. The contractor is expected to perform per defined Quality Assurance Surveillance Plan measures and metrics.

By procuring network security insurance against possible threats, a company transfers cost risk of data being accessed in the event their network is compromised. The company assumes the cost of the insurance, and the overall cost impact of the event is covered by the insurer. However, this does not protect the company’s reputation. In this case only cost is transferred. Impact to individuals because of the data breach may be unavoidable.
1.3.4 MITIGATE

Mitigation is the identification of strategies and steps or activities to minimize the eventuality that a trigger (root cause) will occur.

- By installing anti-virus software on a computer and establishing good monitoring techniques, the risk of malware being loaded or other compromising activity is minimized.

- To mitigate the possibility of slipping on an icy sidewalk, I might wear non-slip soled shoes, spread sand or kitty litter, or eliminate the root cause with ice-melt or an under sidewalk heater. Each opportunity is a step toward minimizing the chance of falling. Each has a cost.

1.4 RISK TYPES

We can identify, classify, and qualify many types of risk in business, IT operations, physical safety, and security sectors. Better, faster, cheaper is often used to describe opportunity costs of project and program risks that deal with performance, cost, and schedule. I can have a good product delivered to market fairly quickly, if I want to spend the dollars for a high number of qualified resources. Or, I can attempt to deliver a product quickly, spend less money by hiring less experienced resources, and run the risk of it not working. If I have the time, I might be able to develop a sound product with less investment dollars by using fewer high quality resources. Choices come with alternative risks including risk to safety and security.

1.4.1 SAFETY

Safety risks involve events that cause harm to people or the environment. On a construction site, hard hats must be worn as a mitigation measure to injury that could be caused by falling debris. OSHA training is required to mitigate or reduce the possibility of accidents that could result from not knowing how to react in certain unsafe situations, like chemical spills and electrical fires. Safety briefs are often held first thing each day to report incidents and alert workers to current environmental conditions.

When flying in turbulent conditions, or at takeoff and landing, the flying public is instructed to remain seated and wear seatbelts. This reduces the likelihood that someone will be injured as the plane bounces or jolts along.

1.4.2 SECURITY

Major security risks involve physical security of a person or property, financial security which might entail savings and retirement investments, and information or cyber security which involves privacy and access to data. People may employ home security systems to reduce risk of home invasion and deter intruders. Anti-virus software and firewalls deter malware and hackers. To ensure one’s ability to continue to support oneself due to lost wages as a result of job loss or in retirement people put money into savings or other investments.

1.4.3 PERFORMANCE

When dealing with project or product performance, look at how the end result or outcomes at appropriate times during each phase meet original requirements and specifications. Does the product or process work as intended and provide the specified desired outcome? A good project will have clearly defined requirements and deliverable expectations, identified roles and responsibilities of any required resources and stakeholders, escalation paths for communication, a realistic schedule, and appropriate funding. Shortchanging adequate competent resources and trying to meet an unrealistic schedule are major contributors to poor contract and product performance. Risks to performance should be identified during planning and appropriate responses outlined prior to project start.

1.4.4 COST

Risks to cost often come from a lack of clearly defined requirements at the onset of a project. Miscalculations in schedule, required resources (human and other), as well as environmental conditions, can all influence cost. A good understanding of requirements and the human or other resources required to deliver those requirements within a realistic timeframe under specified conditions is paramount to maintaining costs from the beginning.
If you are implementing a computer system and other sensitive equipment in an environment that is hot, arid, and subject to heavy wind storms then accommodations for the equipment should be considered to abate risks to damaged equipment. Appropriate cooling and shelter or encapsulation that offers protection from particulate matter (sand and dirt most often) should be considerations during planning. If you are managing a program where these risks are common, then cost of reducing the opportunity, as well as maintenance, repair, and replacement should be budget considerations, in order to maintain the program on a consistent basis. Maintenance cost might be an accepted risk, even though steps to reduce likelihood of occurrence are implemented.

Risks to schedule can be major risks to cost if not planned accordingly. For example, if equipment delivery is delayed then I may need to retain contract staff an additional number of days to complete the project. Or, if software licenses aren’t renewed by a specified date each year, I may incur additional cost to reinstate them.

Failure to communicate market changes and recommend action in a timely manner to clients can result in financial loss to both clients and brokers.

1.4.5 SCHEDULE

A schedule risk is an event that would impede delivery of a product or process fulfillment within a specified time. When planning a program or project, avoid the urgency of schedule outweighing good engineering and program management. A schedule should reflect realistic and event-driven phasing for analysis, communication, systems engineering, integration, test activities, and corrective actions. It is important to plan appropriate resources and schedule margin (lag time) with the flexibility to accommodate unplanned risks and issues. The project plan should be structured to ensure that system performance is demonstrated prior to full financial commitment. For example, don’t order 12 new drones if you haven’t seen the prototype perform per specifications. Maintain appropriate review activities, perform analysis, and institute corrective and preventive actions as warranted.

When budgeting required resources to fulfill project requirements within a specified time, one should explore the risks of human, equipment, and environmental conditions that might cause delays. Plan costs commensurate with program and project complexity. Conduct schedule risk assessments on a regular basis to assess risks and inform mitigation activities associated with achieving milestones. Communicate assessment outcomes to appropriate stakeholders and manage mitigations appropriately.

1.5 RISK OF NOT IMPLEMENTING RISK MANAGEMENT IN AN ORGANIZATION OR PROJECT

We’ve talked about types of risk, risk responses, and what a risk is in general terms. So what happens if we don’t institute a risk management process or plan within our organization or project? Really, do we need to go into detail? Lives may be lost, individuals will live with loss or injury, airlines get sued, employers pay more workers’ compensation and unemployment, businesses lose revenue, airports, borders and ports become less secure and hazardous material (explosives and radioactive contraband) are transported to become weapons of mass destruction, investment accounts fail to meet retirement goals, soldiers die.

© 2015 NORTH STAR GROUP, LLC

© 2015 NORTH STAR GROUP, LLC
2. RISK MANAGEMENT PLANNING

The PMI’s PMBOK, DoD, and FAA as well as other Government, private, and commercial institutions have detailed instructional guidance on risk management planning. The suggestions found in this writing are high level and intended to be used as a starting point to risk management discussion and implementation within organizations and projects. Risk managers should refer to their agency or organization’s risk guidance to ensure compliance when instituting risk management.

2.1 RISK MANAGEMENT IMPLEMENTATION PLAN

The best opportunity for reducing loss is to plan for the eventuality that risks may be realized. Things do go wrong and can be out of your control. Risk planning doesn’t just entail describing risk, assessing root cause and probability and consequence, identifying actions to minimize impact, and logging into risk management tools. Risk planning involves stakeholders, knowing who may be impacted, what and how communications will take place, and who owns and will monitor mitigation steps (corrective and preventive actions) to resolution. It also involves leadership’s understanding and regular review or escalation, so that prompt decisions can be made.

A risk management implementation plan will identify the following:

• Purpose of the plan and leadership authority.
• Scope to include programs, project(s), organization(s), timeframe or period of performance of the plan
• Roles and Responsibilities including subject matter experts and assessment of capabilities of potential sources through early industry involvement
• Tools
• Communication / Escalation Path
• Risk Process and procedures
• Risk Board or Committee and Charter

2.2 PURPOSE

Identify the intent of your risk plan and sponsor or authorizing authority.

2.3 SCOPE

Identify to whom the plan applies. Identify organizations, programs, projects and the types of risks being considered in the plan.

2.4 ROLES AND RESPONSIBILITIES

When planning how risks will be managed within your organization or project take the time to perform a stakeholder analysis. Who will be impacted if a process or product fails? Who owns or supports requirements and the phases of a project to delivery? What functions and activities or tasks does each stakeholder organization play? Are contractor and other industry organizations involved? Who are the leaders and decision makers in those organizations who have the authority to take action?
THE FOLLOWING TABLE IS A SAMPLE STAKEHOLDER ANALYSIS:

<table>
<thead>
<tr>
<th>ORGANIZATION</th>
<th>CONTACT INFO</th>
<th>ROLE</th>
<th>RESPONSIBILITY / FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Management</td>
<td>PH eMail</td>
<td>Requirements sponsor; Funding allocation</td>
<td>Reviews / approves project requirements, works with supporting organizations to validate relevancy, funds project</td>
</tr>
<tr>
<td>Technical Authority</td>
<td>PH eMail</td>
<td>Architects, delivers, monitors, and supports WAN network infrastructure, data and information security measures</td>
<td>Approves engineering designs per specified requirements, monitors network security, takes appropriate action.</td>
</tr>
<tr>
<td>Local Installation</td>
<td>PH eMail</td>
<td>Implements and supports network infrastructure measures as directed by the technical authority. Designs and implements and supports local LAN infrastructure and desktop computing.</td>
<td>“Feet on the street” hands on implementation, maintenance, and support of LAN and desktop computing equipment, including access, capacity, and availability management.</td>
</tr>
<tr>
<td>Field Offices</td>
<td>PH eMail</td>
<td>Users, focused on defense and homeland protection activity. The entity for whom the product is being developed.</td>
<td>Create, store, and use data across the network.</td>
</tr>
<tr>
<td>Contracts, or other acquisition authority</td>
<td>PH eMail</td>
<td>Acquisition / procurement and project management body</td>
<td>Analyzes requirements and procures products and resources per specifications.</td>
</tr>
<tr>
<td>Facilities Management Organization</td>
<td>PH eMail</td>
<td>Owns and supports facilities that house network infrastructure and computing equipment in the continental US.</td>
<td>Physical environment and security of network equipment including heating, cooling, cabling.</td>
</tr>
<tr>
<td>Project Lead</td>
<td>PH eMail</td>
<td>Works with stakeholders to plan requirement analysis, design, development, test, implementation, integration, and product delivery</td>
<td>Plans project with stakeholders, including communication, risk, schedule, and cost management. Oversees all aspects of the project, conducts consistent project meetings, communications, and escalates as necessary.</td>
</tr>
<tr>
<td>Engineering</td>
<td>PH eMail</td>
<td>Designs and develops products and processes</td>
<td>Designs and develops products and processes per approved architecture from technical authority. Conducts phased product and documentation reviews.</td>
</tr>
<tr>
<td>Contractor Support</td>
<td>PH eMail</td>
<td>Design and development support, implements, supports, and maintains as directed by contract.</td>
<td>Design and development support, implements, supports, and maintains as directed by contract.</td>
</tr>
</tbody>
</table>
2.5 TOOLS

Effective tools used in risk management include:

- **Meetings** – a meeting forum provides an optimum collaborative venue for discussion, identification, review, risk mitigation planning, and status updates.

- **Expert judgement** – Risk identification and management require input from a variety of sources: management, stakeholders, project managers, subject matter experts, industry, other professional and technical associations.

- **Risk log / register** – used to capture risk detail. Risk status including transition to issue status is often maintained in the risk log/register. Recommended risk log detail:
  - Project or organization
  - Risk statement (preferably in if then format)
  - Project lead and Organization
  - Risk owner and Organization
  - Customer or key stakeholder(s)
  - Mitigation strategies and steps – A risk may have multiple mitigation strategies. For each strategy in a mitigation strategy identify:
    - Title of mitigation
    - Owner
    - Start / finish date
    - Dependencies
    - Step descriptions
    - Status (capture updates weekly)
    - Automated online reporting

While MS Excel is an excellent tool for tracking, organizations may also choose to utilize a web based tool or other software designed specifically for logging and managing risks. A number of these tools provide assessment capabilities and real time reporting, like dashboards.

2.6 COMMUNICATING RISK

Stakeholders are key players in project planning. Stakeholders need to be informed of risks and participate in the assessment, mitigation and decision making process so that impacts are understood and appropriate responses instituted. The project and risk plan should include a communication element, both horizontal and vertical, that identifies interfaces between organizations and the roles and responsibilities of each in supporting the project and mitigating risks and issues. During planning, frequency and media for communication will also be determined.

2.7 RISK IDENTIFICATION AND MANAGEMENT PROCESS

During the project planning phase, or upon direction by organizational authority, the project or designated risk manager will solicit risk input from stakeholders. Risk identification, assessment, analysis, reporting, review, and planning are iterative processes to ensure resolution and project success. The following table can be used or tailored to identify risk management process steps appropriate for your project or organization.
<table>
<thead>
<tr>
<th>PROCESS STEP</th>
<th>DESCRIPTION</th>
<th>PARTICIPANTS</th>
<th>TOOL(S)</th>
<th>INPUTS</th>
<th>OUTPUTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Identify Risk</td>
<td>Kick-off meeting w/stakeholders and other project participants</td>
<td>• Project Lead • Risk Manager • Subject Matter Experts • Project Participants • Project Stakeholders</td>
<td>• Meetings • Risk Register • Expert Judgement</td>
<td>• Risk Mgt Plan • Cost Mgt Plan • Schedule • Quality Plan • Resource Plan • Stakeholder register • Project Communication Plan • Environmental factors • Procurement documents</td>
<td>• Risk Register</td>
</tr>
<tr>
<td>1.1 Conduct meeting to brainstorm project risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.0 Assess Risks</td>
<td>Perform Qualitative and Quantitative Risk Analysis</td>
<td>• Project Lead • Risk Manager • Subject Matter Experts</td>
<td>• Data gathering • Analysis and modeling techniques • Expert judgement</td>
<td>• Risk register • Risk, cost, and schedule mgt plans • Environmental factors</td>
<td>• Risk cube with numeric probability/consequence rating • Prioritization of project risks • Updated risk register</td>
</tr>
<tr>
<td>3.0 Plan Response / Mitigation</td>
<td>Identify mitigation strategies and steps (we will not focus on transfer, accept, or avoid here)</td>
<td>• All project participants and stakeholders</td>
<td>• Data gathering • Expert judgement</td>
<td>• Risk mtg plan • Risk register • The 5 “whys”, ask why will this occur to each response until origin of event or problem is realized.</td>
<td>• Root cause • Mitigation steps • Updated risk register • Updated risk mtg plan and other project docs • Schedule task inputs • Mitigation owners</td>
</tr>
<tr>
<td>4.0 Monitor and Control Risks</td>
<td>Iterative review and analysis of risk mitigation strategies to optimize outcomes.</td>
<td>• Project Lead • Risk Manager • Project participants • Risk owner</td>
<td>• Risk assessment • Risk audits • Variance and trend analysis • Reserve analysis • Performance measurement</td>
<td>• PMP • Risk register • Work performance data and reports</td>
<td>• Change requests • PMP updates • Updated risk register • Work performance information</td>
</tr>
<tr>
<td>4.1 Risk Management Board Review</td>
<td>Leadership and key stakeholder risk review process to ensure appropriate mitigation, cross organizational escalations, and decisions to address risks.</td>
<td>• Risk Management Board members</td>
<td>• Meeting • Analysis including performance measures • Expert judgement</td>
<td>• Risk report including risk cube and burn down log • Risk register • Change requests • Work performance data and reports</td>
<td>• Approved change requests • PMP updates • Risk register updates • Decisions • Escalation across organizations</td>
</tr>
</tbody>
</table>
2.8. RISK ANALYSIS
(PROBABILITY/LIKELIHOOD AND
CONSEQUENCE/Criticality)

What is the chance that an identified risk will happen? What are the impacts and criticality of the impacts? Both qualitative and quantitative methods can be used to make these determinations. Outputs of qualitative analysis include “updates to the risk register, changes in probability and impacts, risk ranking or scores, risk urgency, risk categorization, and a watch list for low probability risks or risks requiring further analysis.

Assumptions could also change. Outputs of quantitative analysis include: probabilistic analysis of the project that list potential schedule and cost outcomes with confidence levels; probability of achieving cost and time objectives; prioritized list of quantified risks; and trends of the risk analysis results when analysis is repeated using organizational historical information.

2.8.1 DOD ANALYSIS AND RISK REPORTING MATRIX

Below is a DoD risk matrix used to reflect acquisition project risks assessment results for likelihood and consequence with 1 presenting least risk and 5 high risk. Organizations may choose to adopt similar visual reporting aids to represent risk analysis results.

<table>
<thead>
<tr>
<th>Level</th>
<th>Likelihood</th>
<th>Probability of Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Net Likely</td>
<td>~10%</td>
</tr>
<tr>
<td>2</td>
<td>Low Likelihood</td>
<td>~30%</td>
</tr>
<tr>
<td>3</td>
<td>Likely</td>
<td>~50%</td>
</tr>
<tr>
<td>4</td>
<td>Highly Likely</td>
<td>~70%</td>
</tr>
<tr>
<td>5</td>
<td>Next Certain</td>
<td>~90%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level</th>
<th>Technical Performance</th>
<th>Schedule</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>RDT&amp;E</td>
<td>Procurement</td>
</tr>
<tr>
<td>1</td>
<td>Minimal or no consequence to technical performance</td>
<td>Minimal or no impact</td>
<td>Minimal or no impact</td>
</tr>
<tr>
<td>2</td>
<td>Minor reduction in technical performance or supportability can be tolerated with little or no impact on program</td>
<td>Able to meet key dates, slip ≤ months</td>
<td>Budget increase or unit production cost increase $A ≤ $B or % of budget</td>
</tr>
<tr>
<td>3</td>
<td>Moderate reduction in technical performance or supportability with limited impact on program objectives</td>
<td>Minor schedule slip, able to meet key milestones, but with no schedule cost slip ≤ months</td>
<td>Budget increase or unit production cost increase $B ≤ $C or % of budget</td>
</tr>
<tr>
<td>4</td>
<td>Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success</td>
<td>Program critical path affected, slip ≤ months</td>
<td>Budget increase or unit production cost increase $C ≤ $D or % of budget</td>
</tr>
<tr>
<td>5</td>
<td>Severe degradation in technical performance, cannot meet RFP or key technical/supportability threshold, will jeopardize program success</td>
<td>Cannot meet key program milestones, slip ≤ months</td>
<td>Exceeds APB threshold &gt;$D or % of budget</td>
</tr>
</tbody>
</table>
### 2.8.2 FAA ANALYSIS AND RISK REPORTING MATRIX

FAA represents safety risk assessment results using the following risk reporting matrix with 1 being the most severe or highest risk and 5 the least impacting:

<table>
<thead>
<tr>
<th>Severity Likelihood</th>
<th>Minimal (5)</th>
<th>Minor (4)</th>
<th>Major (3)</th>
<th>Hazardous (2)</th>
<th>Catastrophic (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent A</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Probable B</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Remote C</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Extremely Remote D</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Extremely Improbable E</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>

*Risk is high when there is a single point or common cause failure.*
2.9. RISK RESPONSE – MITIGATION PLANNING AND ROOT CAUSE

Mitigation strategies will initially be identified during risk planning and assessment. A good mitigation plan will identify the reason the risk event will occur and provide strategies and identify the tasks needed to reduce likelihood or eliminate the risk or event. Use the “5 whys” to determine root cause, the triggers of an event. The brainstorming team should ask why an action will take place that will cause the event identified to occur? For each response, ask why again. The end result of the process will be the “root” of the risk or issue.

NOTE: it may not take “5 whys”.

Examples:

RISK: “If a company can’t retain qualified personnel, then service levels may not be met”.

- Why?: Because tasks require skill, knowledge, experience and competence to resolve incidents, problems, events, and put preventive and corrective measures in place quickly.
- Why?: Because each event may require varying amounts of time to resolve depending on skill/competence level.
- Why?: Because IT is complex and a higher skilled workforce can respond more accurately quicker. A lower skilled workforce will take longer to identify cause and resolve incidents and problems, if at all.
- Why can’t the company retain the higher skilled staff? Because it bid too low and was awarded a contract which reduced funds for higher skilled experienced workers.

Possible mitigations (each scenario carries its own risks):

1. Reduce service levels (measures for specified task areas) in the quality plan during the bid process based on the knowledge that fewer highly skilled staff will be available.
2. Increase training for staff (trained staff with lower wages will seek higher wages elsewhere).
3. Be realistic in the bid process and justify costs of higher skilled staff for specified service areas and associated retention goals and benefits to the consumer.

RISK: If there is no virus software on a computer, then data may be compromised.

- Why?: Because there are bad guys out there who want information to do bad things.
- Why?: Because access to data can create opportunities?
- Why?: see above

Possible mitigations:

Access to data is the root cause of the issue. Implement protective measures to prevent data from being accessed.

1. Anti-virus software installation
2. Encrypt data
3. Strong password protection
4. Firewalls to inhibit network access

Mitigation strategies are those actions required to reduce risk, prevent triggers and events. These may be entered in the risk register along with the steps or tasks needed to resolve or reduce the risk. These should also be entered in the project schedule to ensure impacts to project deliverables are appropriately identified and tracked.

A “risk burn down” plan may also be developed to track risks through the mitigation process from start to end. A “risk burn down” graph can be used to identify change in likelihood and consequence as each mitigation step is accomplished until the end at which point the risk should no longer be a threat.

2.10. RISK MONITORING

Risks may be reviewed during regularly scheduled project meetings, status updated, and re-planned as warranted. Project schedules should be updated with mitigation steps as tasks and tracked like any normal project task. If the organization has a risk management board or committee, their process should be followed for risk reporting, review, and escalation.
3.0 RISK MANAGEMENT IMPLEMENTATION

An effective risk management program within an organization or project begins with leadership support and enforcement of the process. A common tool used to outline risk management authority and responsibility is the Risk Management Board or Committee Charter.

3.1. RISK MANAGEMENT BOARD OR COMMITTEE CHARTER

The Risk Management Board provides oversight, review, and operates as a decision making authority to ensure appropriate mitigations and escalates across organizations or vertically as warranted. The Risk Management Board process enforces risk management within the organization.

The following outlines sample risk board or committee charter detail:

- **Purpose** – the purpose of the risk board is to ensure regular review, appropriate mitigation, decisions, and escalation of identified risks and issues within an organization or project.

- **Scope** – Describe the span of authority of the board in relation to risks being reviewed.

Risks reviewed are within ABC organization control only. External organizations who have a responsibility for risk mitigation or risk ownership of an ABC lead project will be identified in the risk log for leadership escalation.

- **Board or committee roles and responsibilities:**
  - **Chairperson** – establishes battle rhythm for risk board reviews (schedule and participants), approves agenda content, and leads board meetings, escalates on behalf of the project lead, enforces participation.
  - **Meeting coordinator / facilitator** – works with chairperson to schedule reviews, sends meeting invites with agendas, takes minutes and actions.
  - **Risk manager** – Collects risk detail from tracking/logging media, confirms detail with project lead and participants prior to the risk review meeting. Ensures appropriate format (risk cube, burn down detail) for review.
  - **Project Lead** – Works with the risk manager to ensure detail provided is accurate. Works with project participants and stakeholders to ensure assessments and mitigations are commensurate with the risk.
  - **Project Participants** – Support the project, are in the communication chain, and may own risk or mitigations.
  - **Stakeholders** – May be impacted by the risk, are in the communication chain, and may own risk or mitigations.

- **Tools**

This section identifies risk management tools used by the board, committee, and teams and any access requirements. It details how the tools will be used, accessed and will also state currency of the media being managed. For example:

The A team uses the xyz risk register in Share Point to log, provide assessment detail, display risk cube, risk burn down, and current status information. Data is reviewed and updated each Monday by the A team risk manager, input solicited from appropriate project participants, and data brought current.

To obtain access to the xyz register, login to www://myaccessportal, and complete the participant access request form. Be sure to include your line of business and supervisor’s info for approval.
• **Meeting format and Frequency** – Identify when, where, the time, and how participants will be notified.

The ABC organization will review risks the first Tuesday of every month. Meetings will be held at 0800 in the board room on the 7th floor in the Executive building. A meeting invite with an agenda and list of risks for review will be forwarded in advance. Risk detail will be compiled the week before. Project managers, participants, and stakeholders will have 24 hours prior to the meeting to confirm and modify detail. Unedited detail will be updated during the review.

• **Communication / Escalation Path** – Identify how risks are communicated in the organization, where risk information is maintained, and who to notify or obtain assistance from as risks are identified or changes to reported risks occur.

Risks are to be kept up to date online in the xyz register. Managers and project participants may access risk detail and run reports as needed. A full report will be distributed monthly, within 24 hours of the risk management board review, to project participants and stakeholders.

Stakeholders and participants should notify the identified project lead for a project if concerns arise prior to the monthly risk review. Project leads will escalate as appropriate.

• **Board / Committee Approval/Concurrence** – the board members will sign the charter as acknowledgement and indication of their agreement to participate.

**3.2 MAKING IT HAPPEN!**

Now that you have a basis of understanding of the importance of risk management and how it works, it’s time to put risk management in place in your organization or project! Here are a few recommended steps to help you along the way:

• Identify risk management references used within your organization

• Share this information with your managers and project leads

• Conduct a brainstorming session on how risk management will benefit the business and introduce applicable concepts from this publication and other applicable references

• With management support, communicate intent and invite designated participants to a risk process development session

• Conduct a risk process development session to obtain input from peers, colleagues and stakeholders. Don’t forget to identify resources, roles and responsibilities, and tools you will use to capture and manage risk detail. It’s okay to start small and use Excel.

• Write your risk management process, be sure to incorporate detail from organization and supported agency references

• Write your Risk Management Board charter

• Obtain management / leadership approval to implement

• Socialize and / or train personnel on the risk management process

• Collect initial risk data and establish your risk register/ log process

• Provide support to your team members and colleagues as they learn and become accustomed to managing risks, and on a routine basis to ensure risks are captured and communicated

• Collect risk reporting detail (risk cube, mitigations, and burn down view)

• Set up your first of many reoccurring risk management board meetings

• Conduct meetings!!!

• Reuse steps as necessary until you have a solid program institutionalized for iterative risk management
4.0 ACRONYMS

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>TERM</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATO</td>
<td>Air Traffic Organization</td>
</tr>
<tr>
<td>CMMI</td>
<td>Capability Maturity Model Integration</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>FAA</td>
<td>Federal Aviation Administration</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>PMBOK</td>
<td>Project Management Body of Knowledge</td>
</tr>
<tr>
<td>PMP</td>
<td>Project Management Plan</td>
</tr>
<tr>
<td>QMS</td>
<td>Quality Management System</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedures</td>
</tr>
</tbody>
</table>

6.0 STAKEHOLDER FEEDBACK

Feedback is welcome. Please contact Beth Hughes at North Star Group. bhughes@northstargroupllc.com.

7.0 DISTRIBUTION/COMMUNICATION

This document is accessible to NSG employees and stakeholders. The most current version is located on: <URL>.

---


iii DoD, p10.


v DoD, p79.

vi DOD p22.

vii PMBOK p315.

viii PMBOK p319

ix PMBOK p 333-341.

x DOD p36.

xi FAA p47.